WHAT IS CLAIMED IS:

1. A digital content server capable of transmitting a selected digital data file comprising at least one of a video file and an audio file to a subscriber device via a communication network, said digital content server comprising:

a memory for storing said selected digital data file and a plurality of encryption keys and a plurality of corresponding decryption keys;

a segmentation controller capable of dividing said selected digital data file into a plurality of segments;

an encryption controller capable of encrypting each of said plurality of segments with a selected one of said plurality of encryption keys; and

a transmission controller capable of determining an average bandwidth of said communication network over an N second period and transmitting said plurality of encrypted segments to said subscriber device in an N second period at an average data rate at least equal to said average bandwidth of said communication network and wherein said transmission controller is capable of transmitting said decryption keys to said subscriber device.

2. The digital content server as set forth in Claim 1 wherein said transmission controller is capable of transmitting said stored decryption keys to said subscriber device upon receipt of a verification signal.

3. The digital content server as set forth in Claim 2 wherein said transmission controller receives verification from said subscriber device.

4. The digital content server as set forth in Claim 1 wherein said segmentation controller is capable of adjusting the size of each one of said plurality of segments.

5. The digital content server as set forth in Claim 4 wherein said segmentation controller is capable of adjusting the size of each one of said plurality of segments according to parameters set by said transmission controller.

6. The digital content server as set forth in Claim 5 wherein the parameters set by said transmission controller are one of equal to the average bandwidth and exceed the average bandwidth of said communications network.

7. The digital content server as set forth in Claim 1, wherein said decryption keys are sent to the subscriber device each time the selected file is played and said decryption keys are required only when a predetermined time period elapses between verification checks by said subscriber device.

8. The digital content server as set forth in Claim 1 wherein said encryption controller is capable of compressing each segment prior to encryption.

9. A communication network comprising:

a plurality of subscriber video players capable of receiving digital content files; and

a digital content server capable of transmitting a selected digital data file comprising at least one of a video file and an audio file to a subscriber device via a communication network, said digital content server comprising:

a memory for storing said selected digital data file and a plurality of encryption keys and a plurality of corresponding decryption keys;

a segmentation controller capable of dividing said selected digital data file into a plurality of segments;

an encryption controller capable of encrypting each of said plurality of segments with a selected one of said plurality of encryption keys; and

a transmission controller capable of determining an average bandwidth of said communication network over an N second period and transmitting said plurality of encrypted segments to said subscriber device in an N second period at an average data rate at least equal to said average bandwidth of said communication network and wherein said transmission controller is capable of transmitting said decryption keys to said subscriber device.

10. The communication network as set forth in Claim 9 wherein said transmission controller is capable of transmitting said stored decryption keys to said subscriber device upon receipt of a verification signal.

11. The communication network as set forth in Claim 9 wherein said transmission controller receives verification from said subscriber device.

12. The communication network as set forth in Claim 9 wherein said segmentation controller is capable of adjusting the size of each one of said plurality of segments.

13. The communication network as set forth in Claim 12 wherein said segmentation controller is capable of adjusting the size of each one of said plurality of segments according to parameters set by said transmission controller.

14. The communication network as set forth in Claim 13 wherein the parameters set by said transmission controller are one of equal to the average bandwidth and exceed the average bandwidth of said communications network.

15. The communication network as set forth in Claim 14 wherein said decryption keys are sent to the subscriber device each time the selected file is played and said decryption keys are required only when a predetermined time period elapses between verification checks by said subscriber device.

16. The communication network as set forth in Claim 15 wherein said encryption controller is capable of compressing each segment prior to encryption.

17. A method for transmitting a selected digital data file comprising at least one of a video file and an audio file to a subscriber device via a communications network, comprising the steps of:

dividing said digital data file into a plurality of segments, wherein said segments are adjustable in size;

encrypting each of said plurality of segments with a selected one of a plurality of encryption keys;

storing a plurality of decryption keys corresponding to said plurality of encryption keys; and

transmitting each said encrypted segment via said communications network to said subscriber device at an average data rate at least equal to an average bandwidth of said communications network.

18. The method as set forth in Claim 17 further comprising the step of transmitting said decryption keys to said subscriber device upon receipt of a verification signal.

19. The method as set forth in Claim 18 further comprising the step of adjusting the size of each one of said plurality of segments according to parameters set by said transmission controller wherein the parameters are one of, equal to the average bandwidth and exceed the average bandwidth of said communications network.

20. The method as set forth in Claim 19 further comprising the step of, responsive to a verification signal, transmitting a copy of said stored decryption keys to said subscriber device for decrypting each said encrypted segment.

21. The method as set forth in Claim 20 the steps of:

said subscriber device verifying a predetermined time period of use of said selected digital data file; and

transmitting said decryption keys to said subscriber device only if said time period is exceeded.